# Public Key Infrastructure: From Theory to Implementation

Panel Chairs: W. Timothy Polk, NIST and Donna F. Dodson, NIST

A certificate-based public key infrastructure (PKI) can provide a mechanism to establish trust relationships and obtain security services. The trust relationships may transcend organizational and even international boundaries, even if the parties were previously unknown to each other. The security services supported can include integrity, confidentiality, and non-repudiation. While the technical promise of a PKI is clear, the corresponding operational issues are not as well understood. The purpose of this session is to provide an in-depth view of the issues involved in implementing and maintaining a public key infrastructure.

To support security services on a broad scale for government or industry, a PKI is an appropriate vehicle. However, implementing and maintaining a PKI is unfamiliar territory. How does an agency or company develop a PKI that will support its internal security requirements today and be positioned to integrate with external PKIs as they emerge?

Recent developments provide valuable insight into these questions. Maturing technical specifications should provide future interoperability. Pilot projects have been performed and initial implementations of PKIs are being developed for various branches of the federal government. The Canadian government is currently implementing their own PKI. The lessons learned in these projects can guide others in the implementation of their own PKIs.

The purpose of this panel is to familiarize the audience with standards, interoperability, and implementation issues. Panel members will discuss relevant technical specifications, security policies for PKI supported applications and PKI components, and lessons learned from pilots and current implementations.

This panel may be of interest to parties in both the private and public sectors. This includes project managers, application developers, and security officers in federal agencies and industry who are considering public key infrastructure to support their applications. This panel will be presented in two sessions: Public Key Infrastructure Technology, and Public Key Infrastructure Implementations.

## Public Key Infrastructure Technology

Donna Dodson (NIST), Session Chair

- *An Introduction to Public Key Infrastructure Technology*: Russ Housley, Spyrus
- *Requirements for Digital Signatures and Supporting Services for Financial Applications*: Chris Martin, General Accounting Office
- *An Overview of Public Key Infrastructure Standards*: Warwick Ford, Independent Consultant
- *Minimum Interoperability Specifications for PKI Components*: W. Timothy Polk, National Institute of Standards and Technology

- *Security Considerations When Using X.509 Certificates*: Santosh Chokhani, Cygnacom Solutions, Inc.
- *Linking Digital Signatures with Manual Signatures*: Victor Hampel, Hampel Consulting

## Public Key Infrastructure Implementations

W. Timothy Polk (NIST), Session Chair

- *Federal Public Key Infrastructure Activities*: Patricia N. Edfors, Government Information Technology Services (GITS) Working Group
- *The MISSI Rollout: Lessons Learned*. Donald R. Heckman, National Security Agency
- *NIST Implementation Projects*: Donna Dodson, National Institute of Standards and Technology
- *Security Infrastructure Program Management Office*: Richard Kemp, General Services Administration SI-PMO
- *CommerceNet Security Showcase*: James Galvin, CommerceNet
- *The Canadian Government PKI*: Wynn Redden, Communications Security Establishment